

ABSTRACT

One aspect of the present invention establishes a session key 10
by a receiving unit R transmitting a plurality of quantities for 11
storage in a public repository. A sending unit S: 9

1. retrieves the plurality of quantities; and 6
2. computes and transmits to the unit R a plurality of 10
sender's quantities. 2

The unit R then: 4

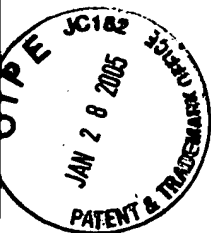
1. computes and transmits to the unit S at least one 10
receiver's quantity; and 3
2. computes the session key. 4

The unit S, using the receiver's quantity, computes the session 10
key. 1

Another aspect provides a digital signature. Before 7
transmitting a signed message, the unit S stores a plurality of 11
quantities in the public repository. A unit R, that receives the 11
message and the digital signature, verifies their authenticity by: 9

1. retrieving the quantities from the repository; 6
2. using the digital signature and the quantities, evaluates 8
expressions in at least two (2) different relationships; 7
and 1
3. verifies the digital signature upon finding equality 9
between evaluation results. 3

Total Words 150



Ref. US 5,581,616
Crandall '616

Claim Text

<p>40. In a protocol for communication in which a sending unit S transmits onto the communication channel I a message "M" together with a digital signature, and,</p> <p>wherein before transmitting the message M and the digital signature, <u>the sending unit S</u> transmits for storage in a publicly accessible repository <u>a plurality of public quantities</u>,</p> <p>a method by which a receiving unit R that receives the message M and the digital signature verifies the authenticity of digital signature</p> <p>comprising the steps performed by the receiving unit R of:</p> <p>a. retrieving <u>the plurality of public quantities</u> from the publicly accessible repository;</p>	<p>Disclosed in the reference.</p> <ol style="list-style-type: none">1. The sender computes a single quantity, ourPub, <u>a particular x-coordinate on the elliptic curve</u>.2. The sender publishes the single quantity ourPub, by storing it into a public source 813. See column 7, line 58 through column 8, line 16.	
<p>a. retrieving <u>the plurality of public quantities</u> from the publicly accessible repository;</p>	<p>Hasher 1206 of the encryption/decryption means 1204 of receiver 1202 receives <u>only a single quantity x-coordinate, "ourPub," from the public source 813</u>. See column 19 at lines 34 through 44.</p>	

Claim Text

<p>b. using the digital signature and the <u>plurality of public quantities</u>, evaluating expressions of at least two (2) different verification relationships; and</p>	<p>One <u>expression</u> is evaluated using:</p> <ol style="list-style-type: none">1. only one part, i.e. P, of the digital signature (u, P);2. the cyphertext message C; and3. <u>the single quantity ourPub</u>, i.e. a particular x-coordinate on the elliptic curve, received from the public source 813. <p>Hasher 1206 recieves the <u>ciphertext message C and point P on the elliptic from nonsecure channel 816 via line 1210, and ourPub from source 813 via line 1218.</u></p> <p>Hasher 1206 outputs point R to comparator 1208 via line 1214. See column 19, lines 40 through 44.</p>	
---	--	--

Claim Text

<p>c. comparing pairs of results obtained by evaluating the expressions of the at least two (2) different verification relationships.</p>	<p>The comparator 1208 receives and compares:</p> <ol style="list-style-type: none"> 1. <u>Q, which is computed by the elliptic multiplier 806 without using any quantity received from the public source 813; and</u> 2. <u>R, which is computed using ourPub which the Hasher receives from the public source 813.</u> <p>The elliptic multiplier 806 of the receiver 1202 receives point u from the nonsecure channel 816. The elliptic multiplier 806 generates point Q and provides it to comparator 1208. Hasher receives the ciphertext message C and point P from the nonsecure channel 816 and the purported senders public key ourPub from source 813 and generates point R, which it provides to comparator 1208. Comparator 1208 compares points Q and R and if they match, the signature is assumed to be valid. See column 20, lines 27 through 37.</p> <ol style="list-style-type: none"> 1) Using the u part of the signature, compute the point $Q = u^*(X_1 / 1)$ <p>See column 26 at lines 53 through 55.</p>
---	---